LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

405(d) Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)

Five Threats Series:
Threat 3 – Loss or Theft of Equipment or Data

April 2019

In Partnership With

The 405(d) Aligning Health Care Industry Security Practices initiative, along with the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication and this engagement are in partnership with the Healthcare & Public Health Sector Coordinating Council (HSCC)

Agenda

Time	Topic	Speaker
5 Minutes	Opening Remarks & Introductions	405(d) Team
5 Minutes	CSA Section 405(d)'s Mandate, Purpose, and Desired Goals	Dan Bowden
5 Minutes	HICP Overview	Dan Bowden
10 Minutes	Using HICP and Supporting Resources	Dan Bowden
40 Minutes	Threat 3 – Loss/Theft of Equipment/Data and Mitigating Practices	Jason Wagner/Dan Bowden
5 Minutes	Looking Forward	405(d) Team
5 Minutes	Upcoming 5 Threats	405(d) Team
15 Minutes	Questions	

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

CSA Section 405(d)'s Mandate, Purpose, and Desired Goals

Cybersecurity Act of 2015 (CSA): Legislative Basis

CSA Section 405

Improving Cybersecurity in the Health Care Industry

- Section 405(b): Health care industry preparedness report
- Section 405(c): Health Care Industry Cybersecurity Task Force
- **Section 405(d): Aligning Health Care Industry Security Approaches**

Industry-Led Activity to Improve Cybersecurity in the Healthcare and Public Health (HPH) Sector

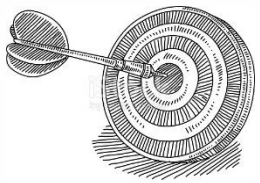
WHAT IS THE 405(d) EFFORT?

An industry-led process to develop consensus-based guidelines, practices, and methodologies to strengthen the HPH-sector's cybersecurity posture against cyber threats.

WHO IS PARTICIPATING?

The 405(d) Task Group is convened by HHS and comprised of over 150 information security officers, medical professionals, privacy experts, and industry leaders.

HOW WILL 405(d) ADDRESS HPH CYBERSECURITY NEEDS?



With a targeted set of applicable & voluntary practices that seeks to cost-effectively reduce the cybersecurity risks of healthcare organizations.

WHY IS HHS CONVENING THIS EFFORT?

To strengthen the cybersecurity posture of the HPH Sector, Congress mandated the effort in the Cybersecurity Act of 2015 (CSA), Section 405(d).

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

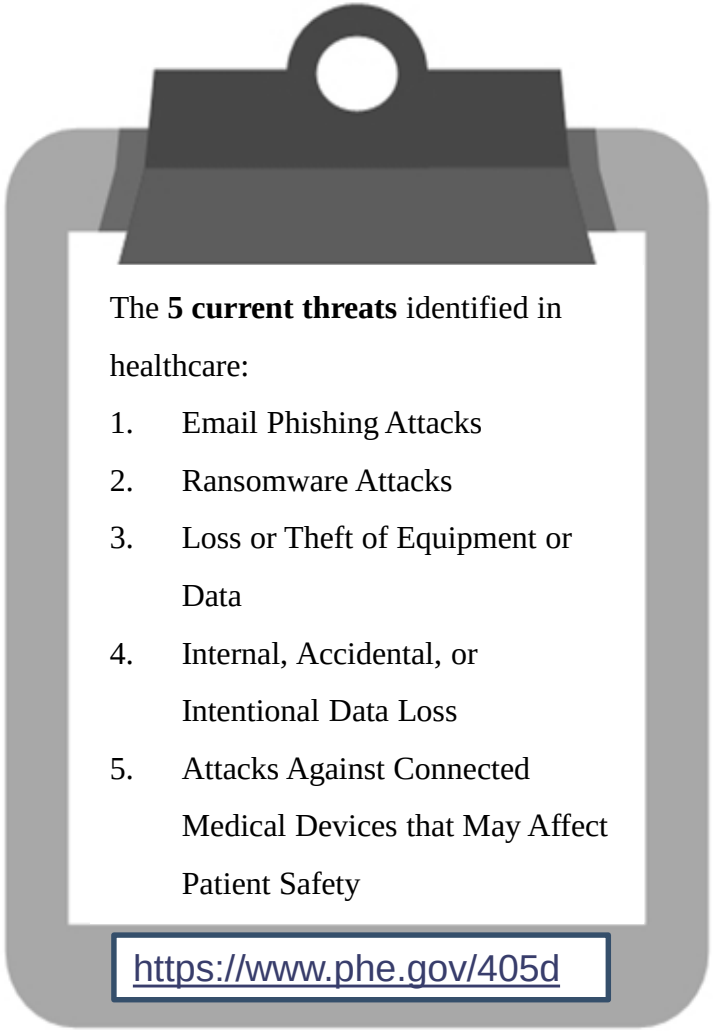
OFFICE OF THE CHIEF INFORMATION OFFICER

HICP Publication Overview

Document - Content Overview (1/2)

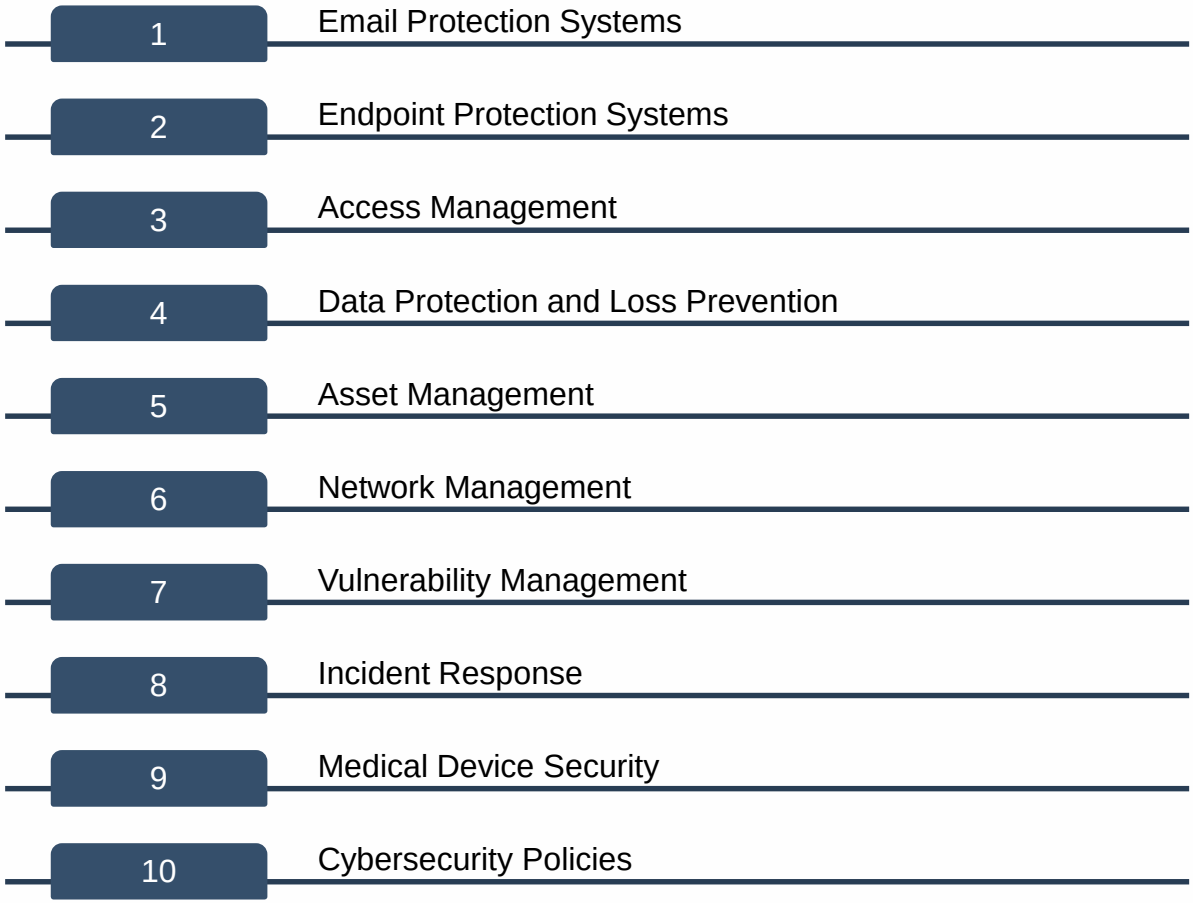
After significant analysis of the current cybersecurity issues facing the HPH Sector, the Task Group agreed on the development of three documents—a main document and two technical volumes, and a robust appendix of resources and templates:

- The main document examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.
- *Technical Volume 1* discusses these ten cybersecurity practices for **small** healthcare organizations.
- *Technical Volume 2* discusses these ten cybersecurity practices for **medium and large** healthcare organizations.
- *Resources and Templates* provides mappings to the NIST Cybersecurity Framework, a HICP assessment process, templates and acknowledgements for its development.



Document - Content Overview (2/2)

The document identifies **ten (10) practices**, which are tailored to small, medium, and large organizations and discussed in further detail in the technical volumes:



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Using HICP and Supporting Resources

Introduction and Executive Summary

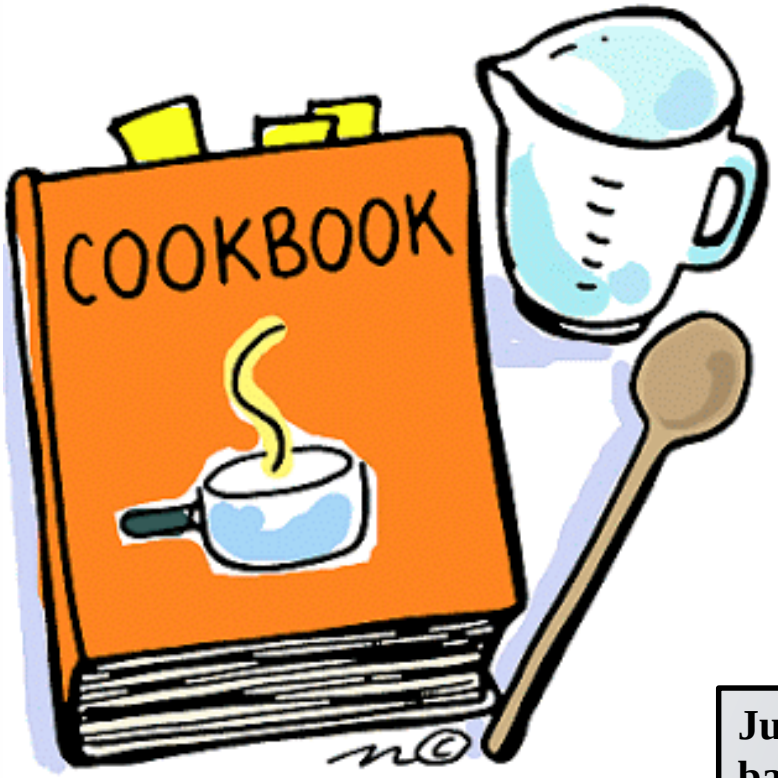
HICP is…

- A call to action to manage real cyber threats
- Written for multiple audiences (clinicians, executives, and technical)
- Designed to account for organizational size and complexity (small, medium and large)
- A reference to "get you started" while linking to other existing knowledge
- Aligned to the NIST Cybersecurity Framework
- Voluntary

HICP is **not**…

- A new regulation
- An expectation of minimum baseline practices to be implemented in all organizations
- The definition of "reasonable security measures" in the legal system
- An exhaustive evaluation of all methods and manners to manage the threats identified
  - You might have other practices in place that are more effective than what was outlined!
- Your guide to HIPAA, GDPR, State Law, PCI, or any other compliance framework

HICP is a Cookbook!



So you want a recipe for managing phishing?

1. 5 oz of Basic E-Mail Protection Controls (1.M.A)
2. A dash of Multi-Factor Authentication (1.M.B)
3. 2 cups of Workforce Education (1.M.D)
4. 1 cup of Incident Response plays (8.M.B)
5. 1 tsp of Digital Signatures for authenticity (1.L.B)
6. Advanced and Next General Tooling to taste (1.L.A)

Preheat your email system with some basic email protection controls necessary to build the foundation of your dish. Mix in MFA for remote access, in order to protect against potential credential theft.

Let sit for several hours, while providing education to your workforce on the new system, and how to report phishing attacks. While doing so, ensure to provide education on how digital signatures demonstrating authenticity of the sender. When finished baking, sprinkle with additional tooling to provide next level protection.

Just like with any cookbook the recipes provide the basic ingredients to making a meal. It does not:

- **Instruct you how to cook**
- **Instruct you on what recipes to use**
- **Limit your ability for substitutions**

The skill of the cook is what makes the dish!

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

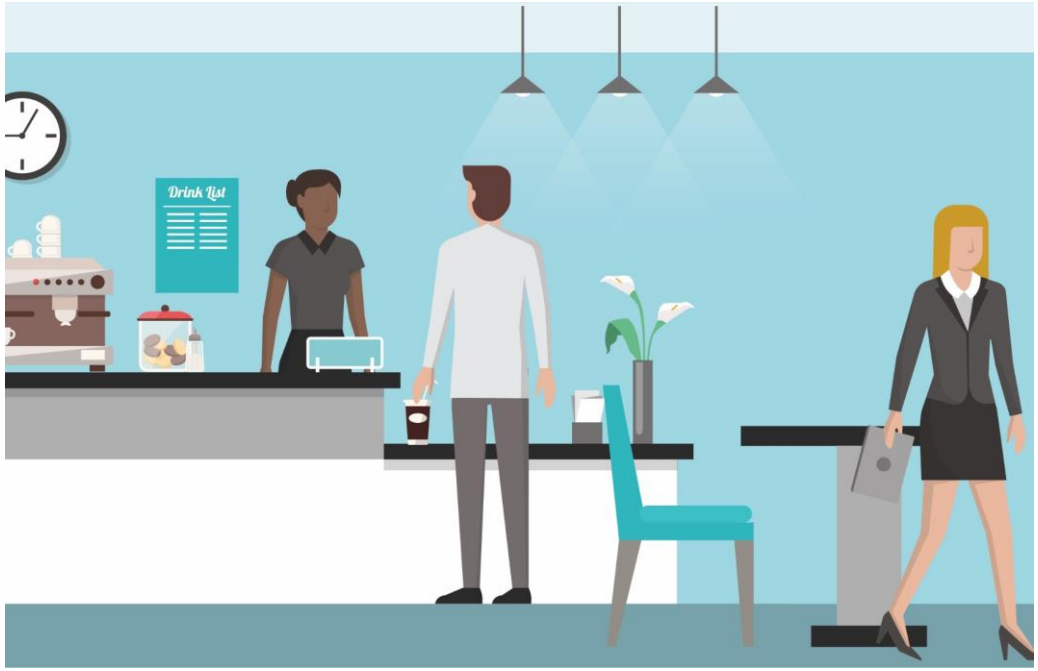
OFFICE OF THE CHIEF INFORMATION OFFICER

Threat 3 – Loss or Theft of Equipment or Data & Mitigating Practices

What is Loss or Theft of Equipment or Data?

Every day, mobile devices such as laptops, tablets, smartphones, and USB/thumb drives are lost or stolen, and they end up in the hands of hackers. Although the value of the device represents one loss, far greater are the consequences of losing a device that contains sensitive data. In cases where the lost device was not appropriately safeguarded or password protected, the loss may result in unauthorized or illegal access, dissemination, and use of sensitive data.

Even if the device is recovered, the data may have been erased and completely lost. Loss or malicious use of data may result in business disruption and compromised patient safety, and may require notification to patients, applicable regulatory agencies, and/or the media.



Loss or Theft of Equipment or Data Scenario

- **Real-World Scenario:** A physician stops at a coffee shop for a coffee and to use the public Wi-Fi to review radiology reports. As the physician leaves the table momentarily to pick up his coffee, a thief steals the laptop. The doctor returns to the table to find the laptop is gone
- **Impact**: Loss of sensitive data may lead to a clear case of patient identity theft, and, with thousands of records potentially stolen, the physician's reputation could be at stake if all the patient records make it to the dark web for sale.

Loss or Theft of Equipment or Data Remains a Challenge

Theft of equipment and data is an ever-present and ongoing threat for all organizations. From January 1, 2018, to August 31, 2018, the Office for Civil Rights (OCR) received reports of 192 theft cases affecting 2,041,668 individuals.

Health care organizations of all sizes need to clearly identify all users and maintain audit trails that monitor each user's access to data, applications, systems, and endpoints. Just as you may use a name badge to identify yourself in the physical work environment, cybersecurity access management practices can help ensure that users are properly identified in the digital environment, as well.

What is Identity and Access Management

Identity and access management (IAM) is a program that encompasses the processes, people, technologies, and practices relating to granting, revoking, and managing user access. Given the complexities associated with health care environments, IAM models are critical for limiting the security vulnerabilities that can expose organizations.

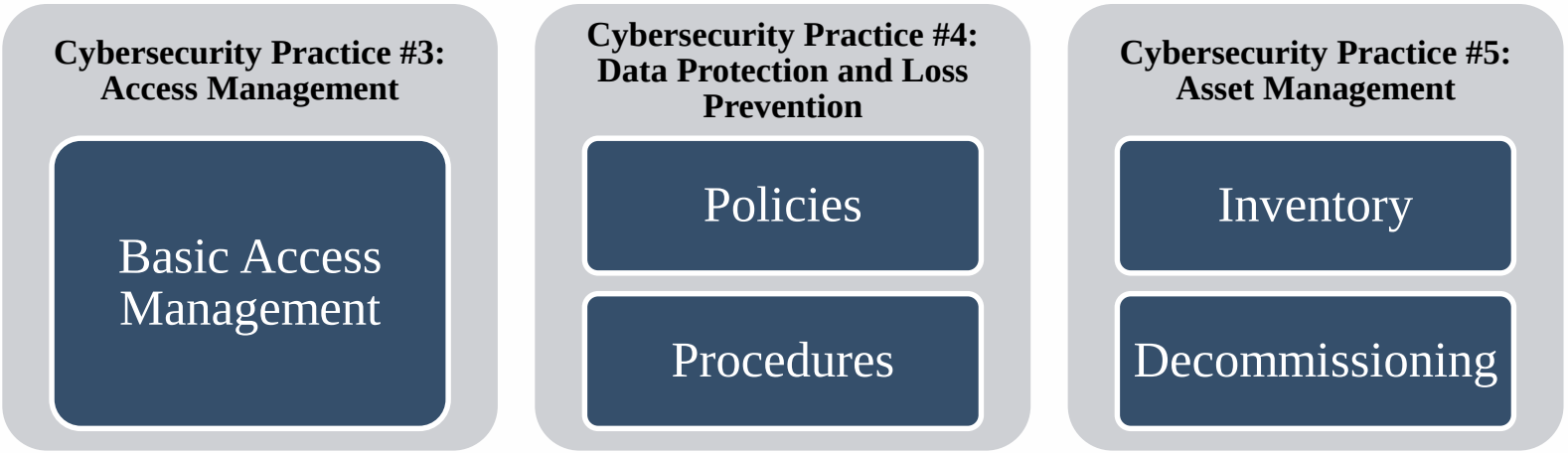
- A common phrase used to describe these programs is *"enabling the right individuals to access the right resources at the right time."*

Cybersecurity Practice 3 provides Identity and Access Management considerations your organization can take to mitigate against Loss or Theft of Equipment or Data

Loss or Theft of Equipment or Data Mitigating Practices - Small Organizations

Technical Volume 1 provides health care cybersecurity practices for small health care organizations. For the purpose of this volume, *small organizations* generally do not have dedicated information technology (IT) and security staff dedicated to implementing cybersecurity practices due to limited resources.

User accounts enable organizations to control and monitor each user's access to and activities on devices, Electronic Health Records (EHRs), e-mail, and other third-party software systems. It is essential to protect user accounts to mitigate the risk of cyber threats. The Loss or Theft of Equipment or Data Mitigating practices in Technical Volume 1 can be found in **Cybersecurity Practice #3, #4, & #5**



Loss or Theft of Equipment or Data Mitigating Practices - Small Organizations

For each Sub-Practice, *Technical Volume 1* provides considerations your organization can take to enhance the security posture

Here an example of what can be found within the sub-practices of **Cybersecurity Practice #3.**

Basic Access Management

Establish a unique account for each user	Assign a separate user account to each user in your organization. Train and regularly remind users that they must never share their passwords.
Limit the use of shared or generic accounts	The use of shared or generic accounts should be avoided. If shared accounts are required, train and regularly remind users that they must sign out upon completion of activity or whenever they leave the device, even for a moment. Passwords should be changed after each use.
Tailor access to the needs of each user	Tailor access for each user based on the user's specific workplace requirements. Most users require access to common systems, such as e-mail and file servers. Implementing tailored access is usually called *provisioning*.
Terminate user access as soon as the user leaves the organization	When an employee leaves your organization, ensure that procedures are executed to terminate the employee's access immediately. This is very important for organizations that use cloud-based systems where access is based on credentials, rather than physical presence at a particular computer.
Provide Role-Based access	Consider following the "minimum necessary" principle associated with the HIPAA Privacy Rule. Allow each user access only to the computers and programs required to accomplish that user's job or role in the organization.

Loss or Theft of Equipment or Data Mitigating Practices - Small Organizations

Here are just a few examples of what can be found within the sub-practices of **Cybersecurity Practice #4 & #5.**

Cybersecurity #4 Sub Practice A: Policies

- Organizational policies should address all user interactions with sensitive data and reinforce the consequences of lost compromised data.
- Establish a data classification policy that categorizes data as, for example, Sensitives, Internal Use, or Public Use. Identify the types of records relevant to each category.

Cybersecurity #4 Sub Practice B: Procedures

- Procedures to manage sensitive data can ensure consistency, reduce errors, and provide clear and explicit instructions. Train your workforce to comply with organizational procedures and ONC guidance when transmitting PHI through e-mail. Encrypt PHI sent via e-mail or text, unless patients expressly authorize their PHI to be e-mailed or texted to them.
- When e-mailing PHI, use a secure messaging application such as Direct Secure Messaging (DSM), which is a nationally adopted secure e-mail protocol and network for transmitting Personal Health Information (PHI).

Cybersecurity #5 Sub Practice A: Inventory

- A complete and accurate inventory of the IT assets in your organization facilitates the implementation of optimal security controls. This inventory can be conducted and maintained using a well-designed spreadsheet. Here are a few examples of they information that should be captured for each device:
  - Asset ID (primary key)
  - Host Name
  - Purchase Order
  - Operating System
  - Media Access Control (MAC) Address
  - IP Address
  - Deployed to (User)
  - User Last Logged On

Loss or Theft of Equipment or Data Mitigating Practices - Small Organizations

Threat 3: Loss or Theft of Equipment or Data | Sub-Practices for Small Organizations			
Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
3 – Access Management	3.S.A Basic Access Management	Promptly report loss/theft to designated company individuals to terminate access to the device and/ or network	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-7
4 – Data Protection and Loss Prevention	4.S.B Procedures	Encrypt sensitive data, especially when transmitting data to other devices or organizations	ID.GV-1, PR.AT-1, PR.DS-2, PR.DS-5, PR.DS-1, PR.IP-6, ID.GV-3
5 – Asset Management	5.S.A Inventory	Maintain a complete, accurate, and current asset inventory to mitigate threats, especially the loss and theft of mobile devices such as laptops and USB/thumb drives	ID.AM-1
	5.S.C Decommissioning	Define a process with clear accountabilities to clean sensitive data from every device before it is retired, refurbished, or resold	PR.IP-6, PR.DS-3

Loss or Theft of Equipment or Data Mitigating Practices for Medium/Large Organizations

Technical Volume 2 provides health care cybersecurity practices for Medium/Large health care organizations. For the purpose of this volume,

- Medium-sized health care organizations generally employ hundreds of personnel, maintain between hundreds and a few thousand information technology (IT) assets, and may be primary partners with and liaisons between small and large health care organizations.
- Large health care organizations perform a range of different functions. These organizations may be integrated with other health care delivery organizations, academic medical centers, insurers that provide health care coverage, clearinghouses, pharmaceuticals, or medical device manufacturers. In most cases, large organizations employ thousands of employees, maintain tens of thousands to hundreds of thousands of IT assets, and have intricate and complex digital ecosystems.

Loss or Theft of Equipment or Data Mitigating Practices - Medium/Large Organizations

The Identity and Access Mitigating Practices in *Technical Volume 2* can be found in **Cybersecurity Practice # 4, #5, & #9**. Medium sub-practices apply to both medium-sized and large organizations. Large sub-practices apply primarily to large organizations, but could also benefit any other organization that interested in adopting them.

Cybersecurity Practice #4: Data Protection and Loss Prevention

- Data Security
- Backup Strategies
- Data Loss Prevention
- Advanced Data Loss Prevention (Large)

Cybersecurity Practice #5: Asset Management

- Decommissioning Assets

Cybersecurity Practice #9: Medical Device Security

- Medical Device Management

Loss or Theft of Equipment or Data Mitigating Practices - Medium Organizations

Here are just a few examples of what can be found within the sub-practices of **Cybersecurity Practice #4 & 5.**

Cybersecurity Practice #4 Sub Practice C: Data Security

- After policies and procedures have been defined, you can establish additional data security methods. The HICP publication provides overviews the following security methods, Encrypting data at rest, encrypting data in transit, Data retention and destruction, and Mask sensitive data within applications

Cybersecurity Practice #4 Sub Practice D: Backup Strategies

- At minimum, each mission-critical asset in your environment should have a backup plan. Backups can be executed using a variety of methods, the most common being disk-to-tape, disk-to-disk, or disk-to-cloud backups. No matter what backup strategy you choose, it is very important to make sure these backup locations are not accessible from the general network or from the general user populations.

Cybersecurity Practice #4 Sub Practice E: Data Loss Prevention

- Once standard data policies and procedures are established and the workforce is trained to use them, DLP systems should be implemented to ensure that sensitive data are used in compliance with these policies.

Cybersecurity Practice #5 Sub Practice D: Decommissioning Assets

- IT assets that are no longer functional or required should be decommissioned in accordance with your organization's procedures. Small organizations often contract with an outside service provider specializing in secure destruction processes. Such providers can ensure that all data, especially sensitive data, are properly removed from a device before it is turned over to other parties. Additionally, your standard operating procedures should ensure that you record the decommissioning of each device.

Loss or Theft of Equipment or Data Mitigating Practices - Medium Organizations

Threat 3: Loss or Theft of Equipment or Data | Sub-Practices for Medium Organizations			
Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
4 – Data Protection and Loss Prevention	4.M.C Data Security	Encrypt data at rest on mobile devices to be inaccessible to anyone who finds the device	PR.DS, PR.DS-1, PR.DS-2, PR.IP-6, PR.DS-5
	4.M.D Backup Strategies	Implement proven and tested data backups, with proven and tested restoration of data	PR.IP-4
	4.M.E Data Loss Prevention	Acquire and use data loss prevention tools	PR.DS-5
5 – Asset Management	5.M.D Decommissioning Assets	Define a process with clear accountabilities to clean sensitive data from every device before it is retired, refurbished, or resold	PR.IP-6, PR.DS-3
9 – Medical Device Security	9.M.A Medical Device Management	Implement a safeguards policy for mobile devices supplemented with ongoing user awareness training on securing these devices	PR.MA-2

Loss or Theft of Equipment or Data Mitigating Practices - Large Organizations

Threat 3: Loss or Theft of Equipment or Data | Sub-Practices for Large Organizations			
Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
4 – Data Protection and Loss Prevention	4.L.A Advanced Data Loss Prevention	Acquire and use data loss prevention tools	PR.DS-5

Loss or Theft of Equipment or Data Mitigating Practices Metrics for Organizations

Specifically for Medium/Large Organizations **Technical Volume 2** contains a series of suggested metrics to measure the effectiveness of the cybersecurity practice. The metrics for **Cybersecurity Practice #4:** Data Protection and Loss Prevention can be found directly following the Sub-Practices for Large Organizations. Here are a few examples of the metrics discussed for Ransomware Attack:

Number of encrypted e-mail messages, trended by week	Number of blocked e-mail messages, trended by week	Number of files with excessive access on the file systems, trended by week	Number of unencrypted devices with access attempts, trended by week
• The goal is to establish a baseline of encrypted messages sent. Be on the lookout for spikes of encryption (which could indicate data exfiltration) and no encryption (which could indicate that encryption is not working properly).	• The goal is to detect large numbers of blocked messages, which could indicate potential malicious data exfiltration or user training.	• The goal is to enact actions that limit access on the file storage systems to sensitive data, create tickets, and deliver to access management.	• The goal is to use this information to educate the workforce on the risks of removable media..

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Looking Forward

Looking Forward

CSA 405(d) aims to be the leading collaboration center of OCIO/OIS, in partnership with relevant HHS divisions, and the healthcare industry focused on the development of resources that help align health care cybersecurity practices

- **Immediate Next Steps**
  - Over the course of the next year the 405(d) Team plans to continue to develop awareness of the HICP publication and engage with stakeholders by:
    - Building additional supporting materials/resources to spotlight the HICP publication and related content
    - Develop means to collect feedback and implementation of HICP practices and methods
    - Hosting additional outreach engagements

Questions

Thank you for Joining Us

Visit us at: www.405d.hhs.gov

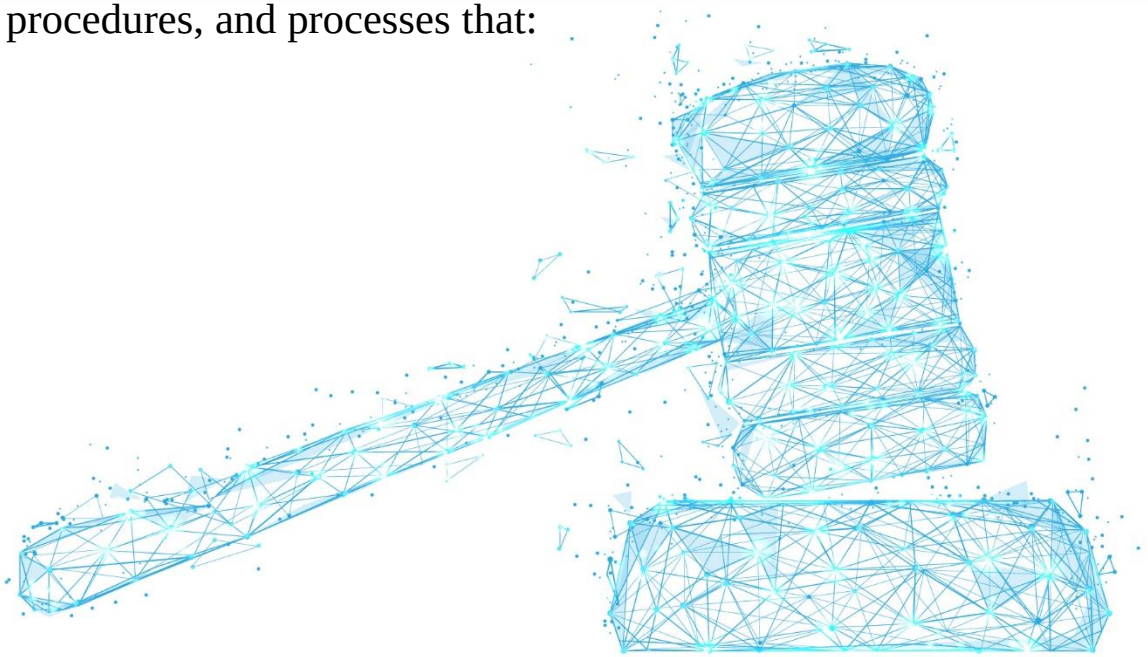
Contact Us at: CISA405d@hhs.gov

APPENDIX

CSA Section 405(d): Legislative Language (1/2)

Authority: Cybersecurity Act of 2015 (CSA), Section 405(d), *Aligning Health Care Industry Security Approaches*

The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that:



CSA Section 405(d): Legislative Language (2/2)

A. Serve as a resource for *cost-effectively reducing cybersecurity risks* for a range of health care organizations;

B. Support *voluntary adoption and implementation* efforts to improve safeguards to address cybersecurity threats;

C. Are consistent with—

   i. The standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)(15));

   ii. The security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note); and

   iii. The provisions of the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111-5), and the amendments made by such Act; and

D. Are updated on a regular basis and applicable to *a range of health care organizations*.

How to Use Practices and Sub-Practices

- There are a total of **10** Cybersecurity Practices, and **89** Sub-Practices.
- Each Cybersecurity Practice has a corresponding set of Sub-Practices, risks that are mitigated by the Practice, and suggested metrics for measuring the effectiveness of the Practice
- Medium Sized orgs can review the Medium Sub-Practices
- Large Sized orgs can review the Medium **and** Large Sub-Practices
- Each Practice is designed to mitigate one or many threats

Cybersecurity Practice 2: Endpoint Protection Systems		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	2.M.A	Basic Endpoint Protection Controls
Large Sub-Practices	2.L.A	Automate the Provisioning of Endpoints
	2.L.B	Mobile Device Management
	2.L.C	Host Based Intrusion Detection/Prevention Systems
	2.L.D	Endpoint Detection Response
	2.L.E	Application Whitelisting
	2.L.F	Micro-segmentation/virtualization strategies
Key Mitigated Risks	• Ransomware Attacks • Theft or Loss of Equipment or Data	

Sample Metrics

- Percentage of endpoints encrypted based on a full fleet of known assets, measured weekly.
- Percentage of endpoints that meet all patch requirements each month.
- Percentage of endpoints with active threats each week.
- Percentage of endpoints that run non hardened images each month.
- Percentage of local user accounts with administrative access each week.

How to Evaluate Your Organization's Size

HICP is designed to assist organizations of various sizes implement resources and practices that are tailored and cost effective to their needs.

- How "large and complex an organization you might be relates to several factors:
  - Health Information Exchanges
  - IT Capability
  - Cybersecurity Investment
  - Size (provider)
  - Size (acute/post-acute)
  - Size (hospital)
  - Complexity
- Determining where you fit is your decision

Medium

[Main Document](), p. 11

Best Fit		Small	Medium	Large
Common Attributes	Health information exchange partners	One or two partners	Several exchange partners	Significant number of partners or partners with less rigorous standards or requirements Global data exchange
	IT capability	No dedicated IT professionals on staff, IT may be outsourced on a break/fix or project-by project-basis	Dedicated IT resources on staff No or limited dedicated security resources on staff	Dedicated IT resources with dedicated budget CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Nonexistent or limited funding	Funding allocated for specific initiatives Potentially limited future funding allocations Cybersecurity and IT budgets are blended	Dedicated budget with strategic roadmap specific to cybersecurity
Provider Attributes	Size (provider)	1–10 physicians	11–50 physicians	Over 50 physicians
	Size (acute / post-acute)	1–25 providers	26–500 providers	Over 500 providers
	Size (hospital)[15]	1–50 beds	51–299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated delivery networks Participate in accountable care organization or clinically integrated network
Other Org Types			Practice Management Organization Managed Service Organization Smaller device manufacturers Smaller pharmaceutical companies Smaller payor organizations	Health Plan Large Device Manufacturer Large pharmaceutical organization

Table 1. Selecting the "Best Fit" For Your Organization

Prioritize Your Threats (with Example)

- Implementing all Practices within HICP could be daunting, even for a Large Sized Organization
- Recommendation: Review the threats and implement the most impactful practices first
  - A toolkit will be released shortly to assist with this process

Factor		
Select your organizations size		Medium
Prioritize the threats (5 being highest priority, 1 being lowest priority)		
A	Email Phishing Attack	1
B	Ransomware Attack	4
C	Loss or Theft of Equipment or Data	5
D	Insider, Accidental or Intentional Data Loss	3
E	Attacks Against Connected Medical Devices that may affect Patient Safety	2

CP #	Cybersecurity Practices	Priority Rank Based on Threat Model Inputs
8	Incident Response	28
3	Access Management	23
2	Endpoint Protection Systems	23
5	Asset Management	20
6	Network Management	16
7	Vulnerability Management	16
10	Cybersecurity Policies	15
1	Email Protection Systems	13
9	Medical Device Security	11
4	Data Protection and Loss Prevention	11

Loss or Theft of Equipment or Data: Direct Mitigating Sub-Practices (S)

The below table lists all of the **direct** Sub-Practices for small organizations to mitigate Threat 3: Loss or Theft of Equipment or Data, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

SP#	SP Title	Short Description
2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable
3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures
4.S.A	Policies	Establishing a data classification policy
4.S.B	Procedures	Procedures for handling sensitive information, pursuant to Data Classification Policy
4.S.C	Education	Training workforce on how to handle sensitive data
5.S.A	Inventory	Conduct and manage an inventory of IT Assets
5.S.B	Procurement	Keep asset inventory up to date with procurement of new devices
5.S.C	Decommissioning	Securely remove devices from the circulation
6.S.B	Physical Security and Guest Access	Physically secure servers and network devices, and segment guest access from regular network
8.S.A	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing

Loss or Theft of Equipment or Data: Indirect Mitigating Sub-Practices (S)

The below table lists all of the **indirect** Sub-Practices for small organizations to mitigate Threat 3: Loss or Theft of Equipment or Data, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

SP#	SP Title	Short Description
8.S.B	ISAC/ISAO Participation	Join an Information Sharing Analysis Center/Organization and receive cyber intel
10.S.A	Policies	Establish cybersecurity policies and a default expectation of practices

Loss or Theft of Equipment or Data: Direct Mitigating Sub-Practices (M)

The below table lists all of the **direct** Sub-Practices for medium organizations to mitigate Threat 3: Loss or Theft of Equipment or Data, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

SP#	SP Title	Short Description
1.M.C	Email Encryption	Use of email encryption for sending sensitive information
2.M.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable
3.M.A	Identity	Establish a unique identifier for all users, leveraging systems of record
3.M.B	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination
3.M.C	Authentication	Implement and monitor secure authentication for users and privileged accounts
4.M.B	Data Use Procedures	Implement data use procedures based upon data classification
4.M.C	Data Security	Implement data protections based upon data classification
4.M.D	Backup Strategies	Backup important data in the case of loss of access, or loss of data
4.M.E	Data Loss Prevention (DLP)	Implement technology and processes to automate security of sensitive data
5.M.A	Inventory of Endpoints and Servers	Establish an asset management inventory database and roll out
5.M.B	Procurement	Keep asset inventory up to date with procurement of new devices
5.M.C	Secure Storage for Inactive Devices	Ensure unused devices are physically secure
5.M.D	Decommissioning Assets	Securely remove devices from the circulation
8.M.A	Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks
8.M.B	Incident Response	Establish formal incident response playbooks for responding to cyber attacks

Loss or Theft of Equipment or Data: Indirect Mitigating Sub-Practices (M)

The below table lists all of the **indirect** Sub-Practices for medium organizations to mitigate Threat 3: Loss or Theft of Equipment or Data, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

SP#	SP Title	Short Description
1.M.B	MFA for Remote Email Access	Enabling multi-factor authentication for remote email access
4.M.A	Classification of Data	Classify data by sensitivity
8.M.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information
10.M.A	Policies	Establish cybersecurity policies and a default expectation of practices

Loss or Theft of Equipment or Data: Direct Mitigating Sub-Practices (L)

The below tables lists all of the **direct and indirect** Sub-Practices for large organizations to mitigate Threat 3: Loss or Theft of Equipment or Data, based upon the HICP publication and the Cybersecurity Practices Assessments Toolkit (Appendix E-1).

SP# = Sub-Practice number
SP Title = Sub-Practice title

Loss or Theft of Equipment or Data: Direct Mitigating Sub-Practices (L)

SP#	SP Title	Short Description
1.M.C	Email Encryption	Use of email encryption for sending sensitive information
2.M.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable
3.M.A	Identity	Establish a unique identifier for all users, leveraging systems of record
3.M.B	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination
3.M.C	Authentication	Implement and monitor secure authentication for users and privileged accounts
4.M.B	Data Use Procedures	Implement data use procedures based upon data classification
4.M.C	Data Security	Implement data protections based upon data classification
4.M.D	Backup Strategies	Backup important data in the case of loss of access, or loss of data
4.M.E	Data Loss Prevention (DLP)	Implement technology and processes to automate security of sensitive data
5.M.A	Inventory of Endpoints and Servers	Establish an asset management inventory database and roll out
5.M.B	Procurement	Keep asset inventory up to date with procurement of new devices
5.M.C	Secure Storage for Inactive Devices	Ensure unused devices are physically secure
5.M.D	Decommissioning Assets	Securely remove devices from the circulation
8.M.A	Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks
8.M.B	Incident Response	Establish formal incident response playbooks for responding to cyber attacks
2.L.A	Automate the Provisioning of Endpoints	Leverage VARs to preconfigure and secure new endpoints
2.L.B	Mobile Device Management	Leverage MDM tools to secure mobile devices
4.L.A	Advanced Data Loss Prevention	Implement advanced technology and processes to automated security of data
5.L.A	Automated Discovery and Maintenance	Leverage automation to keep asset inventory details up to date
5.L.B	Integration with Network Access Control	Catch endpoints on the network that fall out of compliance or are outliers
6.L.E	Network Access Control (NAC)	Ensure endpoints are secure on the network through automated tools

Loss or Theft of Equipment or Data: Indirect Mitigating Sub-Practices (L)

SP#	SP Title	Short Description
1.M.B	MFA for Remote Email Access	Enabling multi-factor authentication for remote email access
4.M.A	Classification of Data	Classify data by sensitivity
8.M.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information
10.M.A	Policies	Establish cybersecurity policies and a default expectation of practices
1.L.A	Advanced and Next Generation Tooling	Advanced email security configurations to enable
2.L.C	Host Based Intrusion Detection/Prevention Systems	Install host based protection systems to detect and prevent client-based attacks
4.L.B	Mapping of Data Flows	Identify and document data storage and data flows between systems
7.L.B	Remediation Planning	Implement formal mechanisms for remediating vulnerabilities and risks